On RSA-Based Signature Standards

John Linn
Principal Architect, RSA Laboratories
June 2000

Presentation Goals and Scope

- **Discuss approaches and harmonization for RSA-based signatures:**
  - Various digital signature methods exist:
    - specifics are non-interoperable
    - standardization, adoption, and deployment vary
  - New techniques reflect advancing state-of-art
- **Emphasizing standards aspects, not mathematics or product features**

RSA LABORATORIES

The Integer Factorization (IF) Family

- **Cryptography based on the difficulty of the integer factorization (IF) problem**
- **Modulus $n = pq$**
- **Public exponent e, private exponent d**
- **RSA: e odd**
- **Rabin-Williams: e even; conditions on p, q**
  - **outside primary scope of this presentation**

RSA LABORATORIES

IF Public-Key Techniques

- **Following IEEE P1363 classification**
- ***Primitives* are mathematical operations on integers, field elements**
- ***Schemes* are sets of operations on messages**
- **Schemes are built up from primitives, “embedding methods” mapping between messages, integers**

RSA LABORATORIES

Notation

M	**message** (string)
m	**message representative** (integer)
s	**signature** (integer)
SP	**Signature Primitive** ($m \rightarrow s$)
VP	**Verification Primitive** ($s \rightarrow m$)

Embedding Methods

- **Mappings between message *M*, integer message representative *m***
  - *Embed*: $M \rightarrow m$
  - *Extract*: $m \rightarrow M$
  - *Check*: M, m consistent?
- **Also called "encoding methods"**
- **Security goals: one-way, collision-resistant, no mathematical structure**

RSA LABORATORIES

Example Schemes in the IF Family

- **Signature schemes with appendix:**
  - **ANSI X9.31**
  - **PKCS #1**
  - **Bellare-Rogaway PSS**
- **Signature schemes with message recovery:**
  - **ISO/IEC 9796-1, 9796-2**
  - **Bellare-Rogaway PSS-R**
- **This talk focuses on the first set**

RSA LABORATORIES

IF Signatures with Appendix

- **Primitives:**
  - SP: $s = m^d \bmod n$
  - VP: $m = s^e \bmod n$
- **Signature operation:**
  - $m = \text{Embed}(M)$
  - $s = \text{SP}(m)$
- **Verification operation:**
  - $m = \text{VP}(s)$
  - $\text{Check}(M, m)$

RSA LABORATORIES

Contemporary Standards

- FIPS 186-2
- PKCS #1
- X9.31

Status of FIPS 186-2

- **FIPS 186-2, Digital Signature Standard (February, 2000), specifies digital signatures using SHA-1 with several types of public-key cryptography**
  - DSA, specified within FIPS 186-2
  - RSA, via ANSI X9.31 or (until mid-2001) PKCS #1
  - Elliptic Curve DSA via ANSI X9.62
- **NIST-accredited program validates implementations**
  - currently, testing available only for DSA; vendor-affirmed conformance possible for other algorithms
  - validation targets both interoperability and assurance aspects

RSA LABORATORIES

PKCS #1: Status

- **PKCS #1 v1.5 (November 1993) defines encryption and signature facilities with ad hoc padding**
  - **widely adopted in industry, Internet standards**
- **PKCS #1 v2.0 (October 1998) defends against encryption attacks (e.g., Bleichenbacher) with Optimal Asymmetric Encryption Padding (OAEP)**
  - **being considered for use with some Internet standards**
- **PKCS #1 v2.1 (draft, September 1999) provides analogous defense against potential signature attacks with Probabilistic Signature Scheme (PSS)**
- **Availability: http://www.rsalabs.com, Internet Informational RFCs 2313 (v1.5), 2437 (v2.0)**

RSA LABORATORIES

PKCS #1 (v1.5): Format and Usage

- **Embed(*M*) =**

  00 01 ff … ff 00 || HashAlgID || Hash(*M*)

- **Ad hoc design**
- **Widely deployed, incorporated in many Internet standards**
  - **PKIX profile**
  - **SSL/TLS certificates**
  - **S/MIME**
- **Being incorporated into IEEE P1363a**

RSA LABORATORIES

PKCS #1: Signature ASN Elements

- pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)}
- md5WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 4 }
- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 5 }
- id-RSASSA-PSS OBJECT IDENTIFIER ::= { pkcs-1 10 }
- RSASSA-PSS-params ::= SEQUENCE {
  hashFunc [0] AlgorithmIdentifier {{oaepDigestAlgorithms}}
  DEFAULT sha1Identifier,
  maskGenFunc [1] AlgorithmIdentifier {{pkcs1MGFAlgorithms}}
  DEFAULT mgf1SHA1Identifier,
  salt OCTET STRING OPTIONAL }

RSA LABORATORIES

ANSI X9.31: Status

- Issued September 1998
- Like PKCS #1 v1.5, uses an ad hoc padding scheme
- Availability: purchase from ANSI
- OID (OIW SecSig, X9.57): {1 3 14 3 2 15}, shaWithRSASignature, intended for use with X9.31 padding
- Intent within X9F1 for document to be reopened to incorporate PSS

ANSI X9.31: Format and Usage

- Embed(*M*) =

  6b bb … bb ba || Hash(*M*) || 3*x* cc

  - where *x* = 3 for SHA-1, 1 for RIPEMD-160
- Ad hoc design
- Incorporated in several standards
  - IEEE P1363, ISO/IEC 14888-3
  - US NIST FIPS 186-1
- Limited industry and Internet adoption

RSA LABORATORIES

X9.31 Constraints on Keys

- **X9.31 requires strong primes, specifies generation techniques**
  - need for strong vs. random primes is controversial
  - adds performance cost and complexity, defends against (some) varieties of trapdoors, particular factoring attacks
- **X9.31 requires modulus sizes in fixed units (1024, 1280, 1536, 1792, 2048, ...)**

RSA LABORATORIES

ANSI X9.31 vs. PKCS #1: Technical Comparison

- Both are deterministic
- Both include a hash function identifier
- Both are ad hoc designs
  - both resist Coron-Naccache-Stern / Coppersmith-Halevi-Jutla attacks on ISO/IEC 9796-1,-2
- PKCS #1 scope concerns format interoperability; X9.31 also imposes constraints on keys
  - PKCS #1 accepts a superset of the RSA keys allowed by X9.31 constraints

Future Directions

- **Probabilistic Signature Scheme (PSS)**
- **Harmonization: issues, status, and a proposed approach**

RSA LABORATORIES

Prudent Security

- **What if a weakness is found in ANSI X9.31 or PKCS #1 signatures?**
  - no proof of security, though designs are well motivated, supported by analysis
  - would be surprising — but so was vulnerability in ISO/IEC 9796-1
- **PSS embodies “best practices,” prudent to improve over time**

RSA LABORATORIES

Bellare-Rogaway PSS

(Probabilistic Signature Scheme, Eurocrypt '96)

- **Embed(M) =**

  $$00 \,\|\, w \,\|\, [\text{Expand}(w) \oplus (r \,\|\, 00 \ldots 00)]$$

  - where w = Hash(r || M), r random
- **Provably secure design**
- **PSS-R variant supports signature with message recovery**

PSS: Standardization Status

- **Standardization of PSS is being pursued in several forums**
  - To be included in IEEE P1363a, PKCS #1 v2.1
  - Intent within X9F1 to reopen X9.31 to incorporate PSS
  - Intent to include PSS-R in rev. to ISO 9796-2
- **Alignment among forums is ongoing**

RSA LABORATORIES

Patent Issues

- **No patents reported to IEEE P1363 for ANSI X9.31, PKCS #1 formatting**
- **PSS embedding method is patent pending by University of California**
  - UC agrees to waive licensing on PSS for signatures with appendix if adopted in IEEE standard (June 15, 1999 letter)
  - informal agreement to extend licensing waiver to other standards bodies
  - "reasonable and nondiscriminatory licensing" for signatures with message recovery

RSA LABORATORIES

Standards vs. Theory vs. Practice

- **ANSI X9.31 is widely standardized**
- **PKCS #1 is widely deployed**
- **PSS is widely considered secure**

- **How to harmonize?**

Challenges

- **Infrastructure changes take time**
  - on the user side
  - in product cycles
- **Specifications vary in scope**
  - complicates modularity among choices
- **Many communities involved**
  - formal standards bodies, IETF, vendors, certificate authorities, validators, ...

Proposed Approach

- **Short term: Continue to support both PKCS #1 and ANSI X9.31 signature formats**
  - e.g., in IETF profiles, FIPS validation
  - continue coexistence until PSS mature, available
- **Longer term: Move toward PSS signatures**
  - not necessarily, but perhaps optionally with "strong primes"
  - upgrade in due course — e.g., along with AES algorithm, new hash functions
- **General: consider decoupling treatment of interoperability vs. assurance characteristics**
  - profile and validate aspects independently?

RSA LABORATORIES